UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/731,509	12/07/2000	Thomas Schaeck	DE919990082	1249

46369 7590 01/11/2007
HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 COLUMBIA CIRCLE
ALBANY, NY 12203

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/731,509	SCHAECK ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-20,22-36,38-43 and 45-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-20,22-36,38-43 and 45-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 10/27/2006, applicant amends claims 16, 19, 28, 32, 34, 35, 41, and 42, and cancels claims 21, 37, and 44. The following claims 16-20, 22-36, 38-43, and 45-47 are presented for examination.

2. Applicant's remarks, filed on 10/27/2006, with respect to the rejection of claims 16-47 have been fully considered but they are not persuasive. Applicant has amended the claims to replace "suppressing involvement of a holder of the card in performing card holder verification" by "performing card holder verification without involving a holder of the card". Applicant indicates that Beuk does not disclose an additional verification (performing card holder verification) as claimed in claim 16. However, Applicant admits on page 10, lines 4-6 that Beuk discloses "If the security code on a given security card does not match the current one in the apparatus memory, the user is asked to enter the correct security code manually" which is also verified. Therefore, there are two verifications one with the card and another with the user entry. Also, the presence of a trusted association can be interpreted as being: whether a card is inserted, or whether the card is a system card or user card, or whether the system code or security code on the card is correct. Applicant argues that Sloan teaches away from card holder involvement (cited in claim 1) and therefore, claim 31 cannot be rendered obvious. Examiner respectfully disagrees because the limitation of controlling association between device and a card has nothing to do with card holder involvement. Also, Applicant's indication in Sloan of "many people prefer not to use PINs" does not prove that the invention of Sloan teaches away from the claimed

invention. The citation does not state "all people". Sloan explicitly states "In one embodiment of the present invention, the issuer of the smart card can also unlock an application" (see column 5, lines 4-6). Column 7, lines 8-11 also discloses "If required (after appropriate identification) the password can be obtained from the card issuer after being easily generated by numerous well-known methods". This clearly shows that Sloan does not teach away from card holder involvement . As shown above, Applicant has not overcome the rejection in view of the prior art. The rejection of claims 16-20, 22-36, 38-43, and 45-47 is set forth below.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 16-20, 22-30, 32-36, 38-43, and 45-47 are rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 5,446,266 to **Beuk et al.**

As per claim 16, **Beuk et al** discloses a method for controlling card holder verification comprising: checking the presence of : whether a card is inserted, or whether the card is a system card, or a user card, or whether the system code or security code on the card is correct for example (see column 2, lines 55-65 and column 3, lines 10-16) that meets the recitation of *checking the presence of a trusted association between at least one device and a card usable*

with the at least one device, and further discloses if any of the above is true, in this instance, a user card is inserted and the system code is checked (see column 2, lines 55-65 and column 3, lines 10-12) that meets the recitation of (*if the checking indicates the presence of the trusted association)* then compare the security code on the card with the currently valid code stored in memory without involving a holder of the card (see column 3, lines 11-16) that meets the recitation of *then performing card holder verification without involving a holder of the card*; *otherwise, if the checking indicates no trusted association* (system code and security code are not correct, column 3, lines 10-11 and 20-22) *then involving the holder of the card in performing card holder verification* (see column 3, lines 21-31).

As per claim 17, **Beuk et al** discloses the claimed method of claim 16, wherein the at least one device is located in a trusted environment (see column 4, lines 1-11).

As per claim 18, **Beuk et al** discloses the claimed method of claim 16, wherein the card comprises a chipcard (see column 1, lines 52-55).

As per claim 19, **Beuk et al** discloses the claimed method of claim 16, wherein the performing card holder verification without involving a holder of the card comprises performing card holder verification hidden from the holder of the card (see column 3, lines 11-16).

As per claim 20, **Beuk et al** discloses the claimed method of claim 19, wherein the performing card holder verification hidden from the holder of the card comprises automatically

obtaining a personal identification number of the holder of the card and verifying the personal identification number without intervention of the holder of the card (see column 3, lines 11-16).

As per claim 22, **Beuk et al** discloses the claimed method of claim 16, wherein the checking the presence of a trusted association between a device of the at least one device and the card comprises comparing a card identifier stored on the card with one or more card identifiers stored in the device (see column 2, lines 55-65 and column 3, lines 10-16).

As per claim 23, **Beuk et al** discloses the claimed method of claim 22, wherein the card identifier is associated with a personal identification number usable in card holder verification, and said method further comprises replacing the personal identification number with another personal identification number (see column 1, lines 36-41).

As per claim 24, **Beuk et al** discloses the claimed method of claim 22, wherein the card identifier is associated with a personal identification number usable in card holder verification, and said method further comprising erasing the association between the card identifier and the personal identification number (see column 1, lines 36-41).

As per claim 25, **Beuk et al** discloses the claimed method of claim 16, wherein the checking the presence of a trusted association between a device of the at least one device and the card comprises comparing an identifier of the device with one or more device identifiers stored on the card (see column 2, lines 55-65 and column 3, lines 10-16).

As per claim 26, **Beuk et al** discloses the claimed method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification, and said method further comprises replacing the personal identification number with another personal identification number (see column 1, lines 36-40).

As per claim 27, **Beuk et al** discloses the claimed method of claim 25, wherein the device identifier is associated with a personal identification number usable in card holder verification, and said method further comprising erasing the association between the card identifier and the personal identification number (see column 1, lines 36-41).

As per claim 28, **Beuk et al** discloses the claimed method of claim 16, wherein the performing card holder verification without involving a holder of the card comprises automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without requesting information from the holder of the card (see column 3, lines 11-16) and wherein the involving the holder of the card comprises requesting the holder of the card to enter the personal identification number (see column 3, lines 27-31).

As per claim 29, **Beuk et al** discloses the claimed method of claim 16, further comprising associating the at least one device and the card (see column 1, lines 53-63).

As per claim 30, **Beuk et al** discloses the claimed method of claim 29, further comprising controlling the association between a device of the at least one device and the card (see column 4, lines 17-22).

As per claim 32, **Beuk et al** discloses the claimed method of claim 16, wherein the checking is between at least one device and a plurality of cards and where in the performing card holder verification without involving a holder of the card is for a plurality of holders (see column 3, lines 38-39, lines 64-68; and column 4, lines 1-17).

As per claim 33, **Beuk et al** discloses a method for performing card holder verification said method comprising: checking the presence of : whether a card is inserted, or whether the card is a system card, or a user card, or whether the system code or security code on the card is correct for example (see column 2, lines 55-65 and column 3, lines 10-16) that meets the recitation of *checking the presence of a trusted association between at least one device and a card usable with the at least one device*, and further discloses if any of the above is true, in this instance, a user card is inserted and the system code is checked then determines if the security code is correct (see column 2, lines 55-65 and column 3, lines 10-15) that meets the recitation of *performing card holder verification based on the checking wherein if the checking indicates the presence of the trusted association* then compare the security code on the card with the currently valid code stored in memory without involving a holder of the card (see column 3, lines 11-16) that meets the recitation of *a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card*;

however, if the checking indicates no trusted association (system code and security code are not correct, column 3, lines 10-11 and 20-22) *then the holder of the card is requested to enter the personal identification number to verify the holder of the card* (see column 3, lines 21-31).

As per claim 34, **Beuk et al** discloses a system of controlling card holder verification, said system comprising at least control device and microprocessor (see column 1, lines 26-36) that meets the recitation of *means for checking the presence of a trusted association between at least one device and a card usable with the at least one device*, for example (see column 2, lines 55-65 and column 3, lines 10-16) **Beuk et al** discloses means for checking the presence of : whether a card is inserted, or whether the card is a system card, or a user card, or whether the system code or security code on the card is correct; and further discloses control device and microprocessor (see column 1, lines 26-36) that meets the recitation of *means for performing card holder verification without involving a holder of the card, if the checking indicates the presence of a trusted association, or for involving the holder of the card in performing card holder verification if the checking indicates no trusted association* (see also column 3, lines 11-16 and lines 21-31).

As per claim 35, **Beuk et al** discloses the claimed system of claim 34, wherein the means for performing card holder verification without involving a holder of the card involvement comprises means for performing card holder verification hidden from the holder of the card (see column 3, lines 11-16).

As per claim 36, **Beuk et al** discloses the claimed system of claim 35, wherein the menas for performing card holder verification hidden from the holder of the card comprises means for automatically obtaining a personal identification number of the holder of the card and verifying the personal identification number without intervention of the holder of the card (see column 3, lines 11-16).

As per claim 38, **Beuk et al** discloses the claimed system of claim 34, wherein the means for checking the presence of a trusted association between a device of the at least one device and the card comprises means for comparing a card identifier stored on the card with one or more card identifiers stored in the device (see column 2, lines 55-65 and column 3, lines 10-16).

As per claim 39, **Beuk et al** discloses the claimed system of claim 34, wherein the means for checking the presence of a trusted association between a device of the at least one device and the card comprises comparing an identifier of the device with one or more device identifiers stored on the card (see column 2, lines 55-65 and column 3, lines 10-16).

As per claim 40, **Beuk et al** discloses a system of performing card holder verification, said system comprising at least one processor (figure 1) to perform card holder verification based on whether a card is inserted, or whether the card is a system card, or a user card, or whether the system code or security code on the card is correct for example (see column 2, lines 55-65 and column 3, lines 10-16) that meets the recitation of *at least one processor to perform card holder verification based on whether a trusted association exists between at least one device and a card*

usable with the at least one device, and further discloses wherein if any of the above is true, in this instance, a user card is inserted and the system code is checked (see column 2, lines 55-65 and column 3, lines 10-12) that meets the recitation of *if the checking indicates the presence of the trusted association* then compare the security code on the card with the currently valid code stored in memory without involving a holder of the card (see column 3, lines 11-16) that meets the recitation of *a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card; however, if the checking indicates no trusted association* (system code and security code are not correct, column 3, lines 10-11 and 20-22) *then the holder of the card is requested to enter the personal identification number to verify the holder of the card* (see column 3, lines 21-31).

As per claim 41, **Beuk et al** discloses an article of manufacture comprising at least one computer usable medium having computer readable program code logic to control card holder verification, the computer readable program code logic comprising: logic to to perform card holder verification based on whether a card is inserted, or whether the card is a system card, or a user card, or whether the system code or security code on the card is correct for example (see column 2, lines 55-65 and column 3, lines 10-16) that meets the recitation of *check logic to check the presence of a trusted association between at least one device and a card usable with the at least one device;* and further discloses comparing the security code on the card with the currently valid code stored in memory without involving a holder of the card (see column 3, lines 11-16) that meets the recitation of *logic to perform card holder verification without involving a holder of the card*; if any of the above is true, in this instance, a user card is inserted and the system

code is checked (see column 2, lines 55-65 and column 3, lines 10-12) that meets the recitation of (*if the checking indicates the presence of the trusted association), or to involve the holder of the card in performing card holder verification* (see column 3, lines 21-31) *if the checking indicates no trusted association* (system code and security code are not correct, column 3, lines 10-11 and 20-22).

As per claim 42, **Beuk et al** discloses the claimed article of manufacture of claim 41 wherein the logic to perform card holder verification without involving a holder of the card comprises perform logic to perform card holder verification hidden from the holder of the card (see column 3, lines 11-16).

As per claim 43, **Beuk et al** discloses the claimed article of manufacture of claim 42, wherein the perform logic comprises obtain logic to automatically obtain a personal identification number of the holder of the card and verify logic to verify the personal identification number without intervention of the holder of the card (see column 3, lines 11-16).

As per claim 45, **Beuk et al** discloses the claimed article of manufacture of claim 41, wherein the check logic to check the presence of a trusted association between a device of the at least one device and the card comprises compare logic to compare a card identifier stored on the card with one or more card identifiers stored in the device (see column 2, lines 55-65 and column 3, lines 10-16).

As per claim 46, **Beuk et al** discloses the claimed article of manufacture of claim 41, wherein the check logic to check the presence of a trusted association between a device of the at least one device and the card comprises compare logic to compare an identifier of the device with one or more device identifiers stored on the card (see column 2, lines 55-65 and column 3, lines 10-16).

As per claim 47, **Beuk et al** discloses an article of manufacture comprising at least one computer usable medium having computer readable program code logic to perform card holder verification, the computer readable program code logic comprising: checking whether a card is inserted, or whether the card is a system card, or a user card, or whether the system code or security code on the card is correct for example (see column 2, lines 55-65 and column 3, lines 10-16) that meets the recitation of *check logic to check the presence of a trusted association between at least one device and a card usable with the at least one device*, and further discloses if any of the above is true, in this instance, a user card is inserted and the system code is checked then determines if the security code is correct (see column 2, lines 55-65 and column 3, lines 10-15) that meets the recitation of *perform logic to perform card holder verification based on the checking wherein if the checking indicates the presence of the trusted association* then compare the security code on the card with the currently valid code stored in memory without involving a holder of the card (see column 3, lines 11-16) that meets the recitation of *a personal identification number of the holder of the card is automatically obtained and verified without requesting information from the holder of the card; however, if the checking indicates no trusted association* (system code and security code are not correct, column 3, lines 10-11 and 20-22)

then the holder of the card is requested to enter the personal identification number to verify the holder of the card (see column 3, lines 21-31).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,446,266 to **Beuk et al** in view of US Patent 6,179,205 to **Sloan**.

As per claim 31, **Beuk et al** substantially discloses the claimed method of claim 30. **Beuk et al** does not explicitly disclose using a network to control the association between the device and the card. Performing the control remotely is an obvious modification and a design choice that only requires routine skill in the art as it allows to perform an operation over a long distance. **Sloan** in an analogous art discloses automatic locking and unlocking application in a smart card without the need of a PIN and further discloses the issuer of the card can generate or

regenerate password of a smart card if a smart card device is unable to do so by having it downloaded into the card holder's personal computer system (see column 5, lines 1-10 and column 8, line 65 through column 9, line 7). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Beuk et al** to allow the control of the association between the device and the card to be done over a network because the advantage is that control may be performed remotely without physical contact with the device and it allows another device located at a different location to change the security code in case the device being present is not capable of doing so as taught by **Sloan** (see column 5, lines 1-10 and column 8, line 65 through column 9, line 7). This modification would have been obvious because one of ordinary skill in the art would have recognized the advantage of allowing an authorized user to change the security code wherever that authorized user is being located as suggested by **Sloan** (see column 5, lines 1-6 and column 7, lines 8-11).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
January 7, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/7/07